Digitalization in Next Generation C2: Research Agenda from Model-Based Engineering Perspective

Jérémy Buisson, Jean Levrai Mbeck M, Nicolas Belloir

Digitalization in Next Generation C2: Research Agenda from Model-Based Engineering Perspective

Jérémy Buisson
Écoles de Saint-Cyr Coëtquidan
CREC / IRISA
Guer, France
jeremy.buisson@irisa.fr

Jean Levrai Mbeck M.
Cameroon Defence Forces
Yaoundé, Cameroon

Nicolas Belloir
Écoles de Saint-Cyr Coëtquidan
CREC / IRISA
Guer, France
nicolas.belloir@irisa.fr

***Abstract*—Since the beginning of the twenty-first century, headquarters and C2 systems of systems have largely evolved in occidental armies, enacting larger distances on the battlefield and increased heterogeneity of units. This evolution combines two related aspects that concern system of systems (SoS) engineering: organizational changes and digitalization. The use of robots and drones, as well as forthcoming next-generation weapon systems will lead to step up this evolution. In this paper, we adopt the model-based engineering perspective to review this foreseeable evolution, in order to identify open challenges.**

***Index Terms*—C2, military SoS, model-based engineering**

I. Introduction

After the introduction of network-centric warfare in the early 2000s, digitalization of the armies is still a challenging concern. The expectations after C2 4.0 (4^{th} generation command and control) programs are mainly to relieve command posts and headquarters from low-value tasks by providing automatic tools in order to let commanders focus on decision making. An underpinning idea is to speed up decision making processes: in the eventuality of high-intensity war against peer enemies, faster making correct decisions is considered a key advantage to seize opportunities and gain initiative.

Digitalization was concomitant with reconfiguration of the (occidental) armies format since the 2000s. These two evolution mutually fostered each other. In addition to the reintroduction of the division level in several occidental armies, the geometry of the battlefield evolved to larger distances, now split in three areas: deep, rear and close. The information flow changes accordingly. On the other side, heterogeneity of units to coordinate is increased, especially with joint and allied operations. As a result, new command structures emerged, including the *command collective* concept, and a three-bureau organization with J5 (future plans), J3/5 (future operations) and J3 (current operations) in the new headquarter [1].

Besides improving decision making and reconfigured organization, current evolution of armed forces exhibit introduction of robots and drones aside warfighters. For instance, a typically armoured platoon will most-probably be composed of a single manned tank, accompanied by two or three unmanned remotely-operated tanks; and each tank will be equipped with several satellite drones to support the mission. All of these units will contribute altogether to fulfill the mission in a single manoeuvre. At lower levels of the command chain, changes expected by C2 4.0 include the ability to design and conduct operations in which parts of the subordinate units are unmanned. Increased autonomy of the equipment, even if still controlled by explicit order, allow to reduce involvement of human warfighters in manoeuvre execution, such that they can be kept at safer positions.

Peer enemies are expected to have similar capabilities. So digitalization brings yet another dimension to the battlefield: the cyberspace. Because of the increased use of digital technologies and networks, command posts and headquarters are not only targets of choice for kinetic attacks, they also become a target for digital weapons. Extension of technology use to the battlefield makes units vulnerable to these new weapons too.

This perspective calls for a new approach to digital orders, beyond the construction of an information system for information centralization and order distribution. This led us to propose a model-driven approach for operation orders [2], i.e., to foster machine-processable format for operation orders.

In this position paper, we further investigate the next generation C2 system of systems, and more precisely how model-based engineering may contribute to military operations, seen as systems of systems. In section II, we review the planning process as implemented by NATO-related nations in their J5 (planning) bureau. Section III focuses on how the J5 bureau reasons about the enemy, in the context of this planning process. Section IV focuses on how friendly forces are taken into consideration. Section V attempts to anticipate foreseeable evolution due to future generations of weapon systems. Section VI gives our concluding remarks.

II. Planning of Operation

In our previous work [2], we proposed a metamodel that provides a structured representation of an operation order (OPORD) as described by NATO's STANAG 2014 [3] standard. But the operation order is just the ultimate product before the operation, that results from the planning process by the so-named J5 bureau.

At NATO level, planning of operations is described by STANAG 2526 / AJP-5 [4], which is refined and adapted

with nation-specific elements such as [5]–[8]. In short, NATO's planning process [4] is a sequence of 7 steps:

1) Initiation: Operation planning initiates when either a political level or higher commander issues a directive for the considered operation. With the help of the command post's staff, the commander issues initial planning guidance, which clarifies the operation and provides key timings. The commander may also issue warning orders to subordinate levels.
2) Mission analysis: By further refinement of the initial planning guidance and by further analysis of upper-level directives, the goal is to formulate the commander's initial intent as well as the overall operation design, including effects, lines of operation and decisive conditions.
3) COA development: Courses of actions (COA) describe how forces and capabilities can be employed in a sequence of actions to achieve the objectives of the mission according to the commander's intent. The intelligence staff first attempts to estimate the most likely and most dangerous adversary's COA. Then the commander calls for imagination to elaborate candidate COA. Only viable (feasible, acceptable, complete, consistent, exclusive and suitable) COA are further refined at the next step.
4) COA analysis: For each presumably-viable COA, advantages and disadvantages are evaluated. Wargaming, i.e., a simplified and targeted simulation of the COA, helps visualize the imagined COA in the context of the foreseen adversary and environment. Troops-to-actions analysis aims at determining capabilities and capacities required by each COA phase.
5) COA validation and comparison: Based on the previous analysis, the commander consolidates the advantages, disadvantages, risks and mitigation for each COA. This consolidated view provides rationale for a list of selected COA, ordered by staff recommendation.
6) Commander's COA decision: The commander chooses one COA, based on staff-provided rationale as well as on personal estimate, experience and judgement. The commander may also choose to alter a COA or to merge several COA in a new single one. The choice acknowledges the commander's acceptance of risks, and gives yet another opportunity to refine the commander's intent. The chosen COA provides a core for the concept of operations (CONOPS) under development at the subsequent step.
7) Plan development: The CONOPS is expected to describe how actions are integrated, synchronized and phased to accomplish the mission, both in space and time. The operation plan (OPLAN) complements the CONOPS to address deployment, employment, protection, support and sustainment in specific annexes.

The resulting OPLAN becomes an operation order (OPORD) when the conditions of execution occur and an execution time is determined [3]. Because this process focuses on planning, feedback like operation debriefing is out of the scope of this process.

To better support the commander and command post's staff in this task, the goal of forthcoming C2 evolution is: shifting from slide-show or natural-language text to structured and computer-exploitable data that enable reasoning like explained in subsequent sections.

One can make an analogy between this NATO's planning process and system engineering processes. In system engineering, the customer starts the project by expressing and justifying the need for the project during an inception phase, matching the initiation step 1. Then the requirement analysis phase helps the system engineer clarify the expectations for the system, like the mission analysis step 2. When properties like safety or security are expected for the system, the engineer performs additional risk analysis tasks, similarly to the analysis of the adversary's COA at the COA development step 3. The system engineer outlines draft architectures, like the COA development step 3 yields to candidate COA. The system engineer usually attempts to early assess how suitable draft architectures are, by means of simulation and analysis. This is almost the same goal as the COA analysis step 4, i.e., to early determine what COA candidates are viable in order to make an informed decision at step 6. Once the system engineer made design decision, she/he pursue development of the architecture, like the plan development step 7. The system architecture is the counterpart of the OPLAN, and the deployment is the counterpart of the OPORD.

In the fields of software engineering and of system engineering, the same shift occurred towards structured and computer-exploitable artifacts. Since then, these fields rely on model-driven engineering technologies, which are intended for this shift. In comparison to other structured data storage, model-based engineering fosters the definition of domain-specific modeling languages with automatic generation of supporting software infrastructure, e.g., [9]–[11]. Model-based technologies provide generic query, transform, analyze tools that can be used with any instance of any domain-specific language.

Obviously the above short comparison between NATO's planning process and system engineering is simplified. Yet it motivates our interest for model-driven engineering.

Challenge: scalability. In the above-described planning process of operations, several artifacts are produced till reaching the ultimate OPORD. Starting from the COA (course of actions), artifacts are built by refinement: the COA serves as the core principles used to elaborate the CONOPS (step 6); which in turn is expanded with function-specific annexes to yield the OPLAN (step 7); which in turn is specialized with actual execution time to become an OPORD (execution of the operation, after planning). At step 3, several COA are attempted and evaluated at steps 4 and 5, which all derive from the initial intent and from the initial planning guidance. All these artifacts are interlinked from the very first step till operation execution, and traceability across artifacts would ensure modeling and tracing the rationale and decisions of

the commander.

The flow between strategic, operational and tactical levels is not unidirectional. Any artifact (CONOPS, OPLAN, OPORD) issued at one level trigger the elaboration of the same artifact at the level below. But at the same time, strategic-level CONOPS benefits from the analysis performed at the operational level. And the operational-level CONOPS benefits from the tactical-level expertise. When artifacts cross the strategic/operational/tactical boundaries, traceability would ensure modeling and tracing the responsibility and decisions of each level's commander.

The above-described planning process accounts only for one level in the command-chain, at a joint, typically theatre level in the case of AJP-5. A similar (simpler) process is applied at lower levels down to platoons, troops to elaborate smaller scale orders for elementary missions. Here again, traceability would ensure modeling and attributing the responsibility and decisions of each level's commander.

These three directions of traceability between artifacts managed in a C2 raise the issue of scaling model-based technologies to large models compound of several artifacts. While scalability is already addressed in persistence layers, e.g., by means of storing models to and querying from various graph-based or column-based databases [12]–[14], scalability to large-scale models is still acknowledged as an open research challenge with respect to infrastructure such as transformation and analysis engines [15].

Challenge: collaborative modeling. In addition to the numerous interlinked artifacts, the above-described planning process involves collaboration. Each commander relies on the command post's staff, which gathers several specialties and expertise. Besides, like already highlighted, collaboration is also involved between strategic/operational/tactical levels. Projects of distributed C2 to improve resilience strengthen this need for collaborative work. In this topic too, proposals already exist in the model-based engineering community, such as [16]–[19]. But Bucchiarone *et al.* [15] note that capturing design alternatives or (possibly contradictory) opinions from the various stakeholders, which may result from a deliberative process like the above-described one, is still challenging.

Challenge: agility. Like acknowledged by the existence of fragmented orders (FRAGO), the OPLAN then OPORD as defined in advance by the J5 (planning) bureau evolves during execution of the operation. Actually, during execution, the process evolves to an agile-like process that enables the commander to seize opportunities, or to react to events even if not anticipated during operation planning. Bucchiarone *et al.* [15] recognize that current model-based technologies intrinsically prevent such agility and evolution in the related processes.

Challenge: multi-domain modeling. Sometimes, a temporary task force is set up with units combining several arms, like the ancient US combat command or the contemporary French GTIA, even when not considering a joint operation. The underpinning idea is that such an organization provides its commander all the expert resources required to fulfill a given mission. Multiple expertise in the staff at the command post is also required to help the commander design annexes to the OPLAN and OPORD, which can be as varied as logistics, signal, air support. Joint operations in addition involve heterogeneous units from any armed forces.

Consequently, the artifacts produced and managed at the command post do not belong to a single mission language. Instead, they are instances of various languages for each domain of expertise. To some extent, this challenge meets the globalized modeling approached [20].

III. Reasoning the Enemy

Reasoning the enemy is about analyzing, then describing the enemy in details: its nature, its attitude, probable doctrine and format/organization in order to take the right decision according to enemy dynamic hypothesis, changeable opinions or views coming from the J2 (intelligence) bureau. The commander should then get a panel of enemy courses of actions highlighting enemy's advantages, vulnerabilities and weaknesses. In the planning process described in section II, reasoning the enemy is key to step 3 and 4 (COA development and analysis) as it tells the commander and its staff most dangerous and most likely actions as well the opponent's center of gravity.

Except the theatre level, units (for instance platoons) do not face the enemy as a whole. Theatre is typically split into areas of interest (AoI) to ensure good coordination between friendly units. Each unit at a given echelon of the command chain splits its own AoI into (smaller) AoI for its subordinated units, which altogether cover the complete AoI of their upper level. Of course, enemy units are spread over the theatre, and like AoI, enemy units are assigned to friendly units to ensure coordination. When reasoning the enemy, each friendly commander has therefore to well identify and to bound his/her own parts of the enemy. Consequently, the commander can discover better focused intention of his/her own enemy, depending on whether this enemy is the one in charge of the main effort, whether this enemy is engaged, either autonomously or with support. Hence the commander has to make the difference between observed enemy's actions and its intention, inferred from the observed actions.

Observing the organization and actions of the enemy is one aspect. Understanding the enemy's military culture and doctrine is mandatory. During COA development and analysis, the command post staff has to think in place of the enemy to anticipate any action that may counter the tentative COA. The enemy's acceptance for risks and casualties, its notion of proportionate use of force affect the enemy's actions and reactions as it defines its favored criteria of choice. Culture, doctrine, but also intellectual formation are therefore key aspects to predict enemy's actions and reactions.

Challenge: help predicting the enemy. When it comes to either recognition or prediction, artificial intelligence (AI) in its various forms provides potential tools. The challenge here is that every enemy has its own military culture and doctrines. Worse, for a given enemy, its military culture and doctrines

may evolve over time. As a result, the corpus of reference data, made of previous wars and battles, may be scarce, small and outdated. For instance, in the context of asymmetric warfare, the enemy may be agile enough to change its COA semiannually (or at a similar time scale), during which new culture and doctrines should be re-inferred or AI should be re-trained before prediction becomes effective again. At the same time, while commanders may be sensitive to deceptive actions, AI faces adversarial examples [21].

Challenge: model of enemy doctrines. Regardless of the use of AI techniques, the commander and command post staff need documented enemy doctrine to try to predict enemy actions. Modeling the corpus of inferred or discovered doctrines by means of model-based techniques would allow machine processing of these doctrines. Indeed, (partial) automation makes the promise of a faster decision cycle, which in turn is expected to provide advantage over the enemy, especially in the context of a peer technologically-advanced enemy. On the one hand, it would enable traceability of CONOPS/OPLAN/OPORD to enemy's doctrines as part of the modeled rationale. On the other hand, model-based doctrines pave the way toward automatic opponent player, e.g., in the context of digitalized wargaming for COA analysis.

IV. Reasoning Friendly Actions

Friendly forces are not only military forces and neighbors or friends, but also those of other stakeholders in the conflict, acting in the battlefield in favor of our commandment. Friendly forces may include civilians, e.g., in the context of civil-military cooperation (CIMIC) and civil-military interaction (CMI). Even out of the scope of CIMIC, civil resources can be used: a typical example is the telecommunication infrastructure. It is acknowledged that military telecommunication technologies is currently lagging behind civil technologies. So, most probably, no military counterpart for 5G mobile networks will ever be developed. Instead, in the near future, military forces will most probably use (possibly hardened) civil 5G equipment, or even civil 5G infrastructure when possible.

In the elaboration of the CONOPS, OPLAN then OPORD like described in section II, the commander needs to know the means at his/her disposal to accomplish the mission. Available means are determined quantitatively, qualitatively, and in terms of suitability to the tasks to be realized. Means are also determined according to their expected evolution during the operation, including soldiers' moral and strength that may vanish as time passes by. As a result, the commander can assess whether necessary resources are available to accomplish the mission, and, if not, request for reinforcements, supplies, support, intelligence, limit updates to increase the global aptitude at his/her disposal.

Challenge: modeling (human) resources. To reason about the friendly forces, resources have to be modeled. System of systems engineering already provides techniques, such as the *physical resource specifications* viewpoints of NAFv4 [22]. In the case of a military operation, some of the resources are human, whose moral, will, tiredness may be affected in the course of the conflict. These specific aspects are unusual in current modeling techniques, even if human beings are present in socio-technical systems as well.

Challenge: unpredictability. Like stated in section III, AI tools based on models for the doctrines and culture can help predict the enemy COA. Likewise, AI tools can provide COA suggestions to the commander, to help faster decision cycle to give advantage. In addition, Yakovleff [23] describes at the tactical level a collection of *coups*, that is, feedback about a sample of manoeuvres that were successful in past conflicts. These *coups* can serve as basis for patterns in the design of the tentative COA for friendly forces. In the context of the friendly forces however, the challenge is to design COA that are hardly predictable by the enemy. Indeed, a peer, technologically-advanced enemy too may have a digitalized C2, including a prediction toolbox similar to the one described at section III, to help discover and anticipate our own friendly actions. So algorithm-assisted decision making must be carefully designed to be sufficiently unpredictable to avoid giving the same advantage as the one provided by a digitalized C2 to a peer enemy.

V. Technological Units

Current trends in weapon systems and their foreseen next generation are headed toward the development of technological units complementing or supplementing human soldiers. This evolution is planned far beyond current Unmanned Ground or Air Vehicles (UGV, UAV), current digitalized battlefield and network-centric warfare. To illustrate, consider the European Main Ground Combat System project (MGCS). A typical MGCS squadron will most probably be composed of few manned armoured vehicles or tanks, and several unmanned, remotely-operated or semi-autonomous armoured vehicles or tanks. Each of these vehicles will be equipped with satellite UGV and UAV. So the MGCS squadron commander will have to command both human soldiers and drone units with reduced crew at disposal.

Similar evolution occurs in the air forces, e.g., with the Future Combat Air System (FCAS) and in naval forces.

Challenge: machine-processable order. In this forthcoming context, because some soldiers are replaced with drone units, any natural-language based format is not suitable anymore, as such orders could not be interpreted nor executed by machines. Model-based representation for orders [2] is a first step to solve the issue. Novel interfaces are required to let small crew command and control the whole squadron. Typical missions and organization of tactical units may evolve as well, hence affecting the language for orders. For instance, the question may arise whether manned vehicles should only remain in the back of the squadron or platoon, or on the contrary be actively involved in the fight. What satellite drones do when their host vehicle is neutralized is an open question that has to be addressed in doctrines as well.

Challenge: cyber-kinetic continuum. The C2 is a key target during conflict, as neutralizing the C2 prevents coordinated conduction of the operation as well as elaboration of new

orders. So neutralizing the enemy C2 may result in complete incapacity of the enemy force. In this context, cybersecurity is mandatory.

Digitalization of the C2 allows new weapons to be used against the C2: digital weapons. Forthcoming weapon systems extends this new opportunity (or risk) to units on the battlefield. Traditional kinetic actions can be complemented (or even substituted) by actions in the cyberspace. As witness of this evolution, the French Ministry of Army publicly claims that digital weapons can be used in coordination with kinetic manoeuvres not only for intelligence, but also to affect or to neutralize enemy's capabilities [24]. Consequently, the current boundary between kinetic battles and cyber battles, which is already blurred, is expected to disappear, hence resulting in a continuum between the spaces in the same way as in current joint operations.

VI. Conclusion

The C2, command post and headquarter are expected to greatly evolve in the future. After network-centric warfare and digitalized battle space started in the 2000s, this evolution is pushed by technological advances, promises made by AI technologies, and forthcoming weapon systems such as European MGCS and FCAS programs. This evolution towards digitalized C2 shifts from a medium between human commanders and soldiers, to integrating decision-assistance technologies, as well as human-to-machine command and control. The digital artifacts that will support an operation are going to be numerous, to refer to global artifact documenting enemy and/or friendly doctrines, and to evolve in the course of the conflict.

Model-based engineering is known to provide basis to address such challenges. This is the reason why, in this position paper, we adopt this perspective to review the forthcoming C2 evolution. Nevertheless, like acknowledged by Bucchiarone *et al.* [15] model-based technologies are still known to raise fundamental questions. Even if scalability and multi-domain modeling have already been studied, model-based technologies are not yet fully satisfying in this regard. Collaborative processes and agility are still open challenges. Finding suitable metamodels, especially to enable doctrine models as well as to take into account human aspects is yet to be done. In addition to foreseeable doctrinal evolution to take into account forthcoming weapon systems, cybersecurity issues are expected to become more pregnant, both on the defensive side and as a new arsenal against a peer enemy, both at the C2 and at the battle field. Last, digitalization is related to the use of algorithms, which raise questions about the undesired predictability of the operations.

Acknowledgment

We would like to thank Stéphane Taillat, from Écoles de Saint-Cyr Coëtquidan, for his comments and suggestions.

References

[1] A. King, *Command: the twenty-first-century general*. Cambridge University Press, Jan. 2019.

[2] N. Belloir, J. Buisson, and O. Bartheye, "Metamodeling NATO Operation Orders: a proof-of-concept to deal with digitalization of the battlefield," in *2019 14th Annual Conference System of Systems Engineering (SoSE)*, May 2019, pp. 260–265.

[3] "STANAG 2014: Formats for Orders and Designation of Timings, Locations and Boundaries," NATO Military Agency for Standardization, Tech. Rep. MAS(ARMY)0307-TOP/2014, Oct. 2000.

[4] "Allied Joint Doctrine for the planning of operations, Edition A Version 2," NATO Standardization Office, Allied Joint Publication AJP-5, May 2019. [Online]. Available: https://nso.nato.int/nso/zPublic/ap/PROM/AJP-5%20EDA%20V2%20E.pdf

[5] P. Fouyet, "Anticipation et planification stratégiques," CICDE, Doctrine interarmées DIA-5(B)_A&PS(2013) 134/DEF/CICDE/NP, Jun. 2014. [Online]. Available: https://www.cicde.defense.gouv.fr/images/documentation/DIA/20130716-NP-CICDE-DIA-5B-APS-2013-AM-23-06-2014.pdf

[6] ——, "Planification du niveau opératif: Guide méthodologique," CICDE, Publication interarmées PIA-5(B)_PNO(2014) 152/DEF/CICDE/NP, Jun. 2014. [Online]. Available: https://www.cicde.defense.gouv.fr/images/documentation/PIA/20140626-NP-CICDE-PIA-5B-PNO-2014.pdf

[7] "Joint Planning," Joint Chiefs of Staff, Joint Publication JP 5-0, Jun. 2017. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

[8] "Allied Joint Doctrine for the planning of operations, Edition A Version 2, with UK national elements," UK Ministry of Defence, Allied Joint Publication AJP-5, May 2019.

[9] S. Gérard, C. Dumoulin, P. Tessier, and B. Selic, "Papyrus: a UML2 tool for domain-specific language modeling," in *Proceedings of the 2007 International Dagstuhl conference on Model-based engineering of embedded real-time systems*, ser. MBEERTS'07. Dagstuhl Castle, Germany: Springer-Verlag, Nov. 2007, pp. 361–368.

[10] D. Steinberg, F. Budinsky, M. Paternostro, and E. Merks, *EMF: Eclipse Modeling Framework 2.0*, 2nd ed. Addison-Wesley Professional, 2009.

[11] J.-P. Tolvanen and S. Kelly, "MetaEdit+: defining and using integrated domain-specific modeling languages," in *Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications*, ser. OOPSLA '09. Orlando, Florida, USA: Association for Computing Machinery, Oct. 2009, pp. 819–820. [Online]. Available: https://doi.org/10.1145/1639950.1640031

[12] A. Benelallam, A. Gómez, G. Sunyé, M. Tisi, and D. Launay, "Neo4EMF, A Scalable Persistence Layer for EMF Models," in *Modelling Foundations and Applications*, ser. Lecture Notes in Computer Science, J. Cabot and J. Rubin, Eds. Springer International Publishing, 2014, pp. 230–241.

[13] X. De Carlos, G. Sagardui, A. Murguzur, S. Trujillo, and X. Mendialdua, "Model query translator: A model-level query approach for large-scale models," in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, Feb. 2015, pp. 62–73, iSSN: null.

[14] G. Daniel, G. Sunyé, A. Benelallam, M. Tisi, Y. Vernageau, A. Gómez, and J. Cabot, "NeoEMF: A multi-database model persistence framework for very large models," *Science of Computer Programming*, vol. 149, pp. 9–14, Dec. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167642317301600

[15] A. Bucchiarone, J. Cabot, R. F. Paige, and A. Pierantonio, "Grand challenges in model-driven engineering: an analysis of the state of the research," *Software and Systems Modeling*, vol. 19, no. 1, pp. 5–13, Jan. 2020. [Online]. Available: https://doi.org/10.1007/s10270-019-00773-6

[16] C. Debreceni, G. Bergmann, M. Búr, I. Ráth, and D. Varró, "The MONDO collaboration framework: secure collaborative modeling over existing version control systems," in *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*, ser. ESEC/FSE 2017. Paderborn, Germany: Association for Computing Machinery, Aug. 2017, pp. 984–988. [Online]. Available: https://doi.org/10.1145/3106237.3122829

[17] S. Kelly, "Collaborative Modelling with Version Control," in *Software Technologies: Applications and Foundations*, ser. Lecture Notes in

Computer Science, M. Seidl and S. Zschaler, Eds. Cham: Springer International Publishing, 2018, pp. 20–29.

[18] D. Kuryazov, A. Winter, and R. Reussner, "Collaborative Modeling Enabled By Version Control," in *Modellierung 2018*, I. Schaefer, D. Karagiannis, A. Vogelsang, D. Méndez, and C. Seidl, Eds. Bonn: Gesellschaft für Informatik e.V., 2018, pp. 183–198. [Online]. Available: https://dl.gi.de/handle/20.500.12116/14938

[19] C. Debreceni, G. Bergmann, I. Ráth, and D. Varró, "Enforcing fine-grained access control for secure collaborative modelling using bidirectional transformations," *Software & Systems Modeling*, vol. 18, no. 3, pp. 1737–1769, Jun. 2019. [Online]. Available: https://doi.org/10.1007/s10270-017-0631-8

[20] B. Combemale, J. DeAntoni, B. Baudry, R. B. France, J.-M. Jézéquel, and J. Gray, "Globalizing Modeling Languages," *Computer*, vol. 47, no. 6, pp. 68–71, Jun. 2014.

[21] N. Carlini and D. Wagner, "Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods," in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, ser. AISec '17. Dallas, Texas, USA: Association for Computing Machinery, Nov. 2017, pp. 3–14. [Online]. Available: https://doi.org/10.1145/3128572.3140444

[22] Architecture Capability Team, "NATO Architecture Framework, version 4," NATO, Tech. Rep., Jan. 2018. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_157575.htm

[23] Michel Yakovleff, *Tactique théorique*, 3rd ed., ser. Stratégies & Doctrine. Economica, Jun. 2016. [Online]. Available: https://www.economica.fr/livre-tactique-theorique-3e-ed-yakovleff-michel,fr,4,9782717867473.cfm

[24] "Éléments publics de doctrine militaire de lutte informatique offensive," Jan. 2019, French only. [Online]. Available: https://www.defense.gouv.fr/english/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf